# 

## United States Patent [19]

Renaud

Patent Number: 1111 Date of Patent:

6.021.491 \*Feb. 1, 2000

[54] DIGITAL SIGNATURES FOR DATA STREAMS AND DATA ARCHIVES

[75] Inventor: Benjamin J. Renaud, Woodside, Calif.

[73] Assignce: Sun Microsystems, Inc., Palo Alto, Calif.

|\* | Notice: This patent issued on a continued prosccution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: 08/753,716

[22] Filed: Nov. 27, 1996

4 SEW USEL 11/1/092 Discour et al

[51] Int. CL7 .. [52] U.S. Cl. ... ...... 380/4, 25 1581 Field of Search ......

[56]

## References Cited

#### U.S. PATENT DOCUMENTS

4,981,370	1/1991	Dziewit et al 380/25
5,005,200	4/1991	Fischer
5.031,214	7/1991	Dziewit et al
5,163,091	11/1992	Graziano et al
5,191,613	3/1993	Graziano et al
5,457,746	10/1995	Dolphin
5,499,294	3/1996	Friedman 380/10
5,572,590	11/1996	Chess 380/4
5,572,673	11/1996	Shurts
5,619,571	4/1997	Sandstrom et al
5,625,693	4/1997	Rohatgi et al 380/23
5,673,316	9/1997	Aperback et al 380/4
5,677.953	10/1997	Dolphin
5,703,951	12/1997	Dolphin 380/25

OTTION PUBLICATIONS

"Public-Key Digital Signature Algorithms", Applied Cryp tography, 2nd Edition, ISBN 0-471-11709-9. Cryptologe Containers: A White Paper, downloaded from www.cryptolope.ibm.com/white.htm on 1ch. 27, 1997. Cryptologic Containers in the News, downloaded from www.cryptolope.iban.com/press.htm on Feb. 27, 1997.

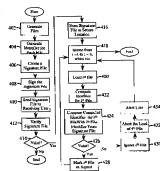
About Cryptologe Containers, downloaded from www.cryptologic.ibm.cum/abrint.htm on Feb. 27, 1997. Primary Examiner-Tod R. Swann

Assistant Examiner-Took! Jack Attorney, Agent, or Firm-Royer & Weaver, LLP

1571 ABSTRACT

Methods, apparatuses and products are provided for verifying the authenticity of data within one or more data files. Each data file is provided with an identifier, such as a one-way hash function or cyclic redundancy checksum. A signature file, that includes the identifiers for one or more data files, is provided with a digital signature created with a signature algorithm. The data file(s) and signature file are then transferred, or utherwise provided to a user. The user verifies the digital signature in the signature file using a signature verifying algorithm. Once verified as being authentic, the signature file can be used to verify each of the data files. Verification of the data files can be accomplished by comparing the identifier for each data file with the corresponding identifier in the signature file. If the identitions in the data and signature files match, then the data file can be marked as authentic. If the identifiers do not match then the data file can be rejected or otherwise dealt with accordingly.

### 13 Claims, 3 Drawing Sheets



178/22.1